IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:	Philip R. Graham
Serial No.	09/733,537
Confirmation No.	1789
Filed:	December 7, 2000
Examiner:	Brandon S. Hoffman
Group Art Unit:	2136
For:	COPY PROTECTION BUILT INTO A NETWORK INFRASTRUCTURE

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

DECLARATION TO OVERCOME A REFERENCE (37 C.F.R. 1.131)

1. The person making this declaration is Philip R. Graham, the inventor of the above-referenced patent application ("Application").

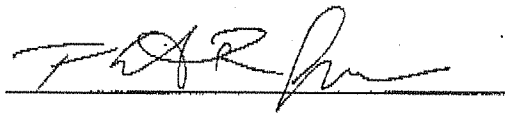
2. This declaration is to establish constructive reduction to practice of the invention in the Application, in the United States, at a date prior to August 8, 2000, that is the priority date ("Priority Date") of U.S. Patent Number 6,732,180 to Hale ("Hale").

3. To establish the date of constructive reduction to practice of the invention of this application, the following attached document is submitted as evidence in redacted form:

Exhibit A. Relevant pages (2 total) from the invention disclosure which was originally submitted to the Assignee of the present application for review prior to the Priority Date of Hale.

4. Exhibit A evidences that the invention in this application was conceived at least by a date that is earlier than the Priority Date of Hale, and that due diligence in preparing and filing the application was exercised from prior to said Priority Date to the filing of the Application.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.



Dated: March 26, 2008

Philip R. Graham

Idea Details (#86861)

Main menu | Reports | Find | Contact | Help Search

Edit Print View Watch Patent Details Review

Copy protection built into a network infrastructure

CPOL No.: 86861 | Seq No.: 3251 | Status: Pending | Submitted: [redacted]

Background: In looking at the current state of entertainment that are rapidly moving to digital forms it becomes easier and easier for individuals to abuse the copyright of the material. As broadband connections become more available it will be easier to copy digital versions of music, video, film and books. These start off as some form of purchased entertainment such as a CD, DVD, Video-tape, digital book etc. People can take these items and with software that is easily located on the internet convert them to alternative digital formats that may have reduced the value of the content (lower quality) or just made it easier to transfer the content to another person which may infringe on the original copyright holders rights. Generally most solutions to this problem involve encription at the edge devices. Both when the content is created and when it is played back. The problem with these types of solutions is that generally it is easy to break this security and remove it from the work trying to be protected. Those systems may still necessary to ensure the highest level of protection. Another problem similar to the above problem is that enterprises and service providers wish to protect their networks from traffic types that could disrupt service to ensure that their customers get the best service from the network that they use. Currently the network administrator has nearly no tools for the mangement of network traffic based on the actual data being transmitted/received. Since the web is so critical to most businesses many applications push their data via http and a well known port used for web traffic (port 80). As a result traditional firewall systems have little effect in the current network systems.

Summary: Two possible solutions to these problems.
1) The concept is to apply digital signatures to data such that the author can be traced. Digital versions of music, video, film, photographs, artwork and books come in a finite number of formats. Formats such as MP3, MPEG-1, MPEG-2, MPEG-4, WMT, Real, GIF, JPEG, can be well understood by the network. The invention is to add software and/or hardware to network equipment such as routers, switches, cache engines, etc that understands these formats and can restrict the flow if the material does not contain the appropriate digital signature then that specific traffic will not to be forwarded under any circumstances.

Creation of content would include a new step which is the incorporation of your digital ID to content that you
create/author. To get this digital ID the person would register with a firm offering this service, the firm would validate your information before giving you this digital ID. Then you could use this ID to be embedded with the content. With the digital ID in place the network equipment would pass the content to whomever you desired. If someone takes copyrighted material and appends their own digital ID such that the network would allow transmission of the content the copyright holder could take obtain the digital ID from the file and deturmine who violated the copyright and take appropriate action.

2) The second solution would have network infrastructure, such as routers, switches, caches look deep into the network packet and allow the network administrator to configure the equipment to not pass specific data types. Examples are MP3 files, MPEG video files, Word Documents, etc... Anything with a file type could be restricted.

Work would be needed to continue to update the file types... Certainly, some will work to hide information from this detection approach, but if they do this then they have to put metods into place that will be widely adopted.

If the digital signature process is easily available and network administrators
do not abuse this tool, then these problems will be minimal.

Advantages: This gives the copyright holder and additional tool to tracking copyright of
their material. Existing methods require end-node support and since end-nodes are open to attach generally copyprotection at the end-node does not stand the test of time.

The Second method allows the network administrator to better control the network traffic in a way that can improve the network performance to reduce undesired traffic types.